IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPELLANT:	Alan Ray Albrecht
SERIAL NO.:	10/620,109
FILED:	July 15, 2003
CONFRM. NO.:	8617
FOR:	OUTPUT PORT BASED DOUBLE Q TAGGING
ART UNIT:	2416
EXAMINER:	Pawaris Sinkantarakorn
DOCKET NO:	200310882-1

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

DATE OF DEPOSIT: <u>April 27, 2009</u>

I hereby certify that this paper or fee (along with any paper or fee referred to as being attached or enclosed) is being submitted on the date indicated above via:

☒ EFS Web
☐ facsimile to _____
☐ the United States Postal Service with sufficient postage as first class mail addressed to: Mail Stop _____, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

/Steve M. Perry/
_____
Steve M. Perry

APPELLANT'S APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Mail Stop Appeal Brief – Patents

Sir:

Appellant submits this Appeal Brief in connection with their appeal from the final rejection of the Patent Office, mailed November 26, 2008, hereinafter "Office Action," in the above-identified application. A Notice of Appeal was filed on February 26, 2009.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS AND INTERFERENCES

Appellant and Appellant's legal representatives know of no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-8, 10-12, 14, 16, and 19 are pending. Claims 9, 13, 15, 17, and 18 were

previously cancelled. Claims 1-8, 10-12, 14, 16, and 19 were rejected by the

Examiner. The claims on appeal in this application are claims 1-8, 10-12, 14, 16, and

19.

IV. STATUS OF AMENDMENTS

No amendments to the presently pending claims have been made since the Office

Action mailed on November 26, 2008, and all the claim amendments have been

entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In claim 1, a method is provided for processing a packet sent to a provider network (page 1, lines 23-24). The method can include receiving the packet via a first user port at a first edge switch of the network (page 1, lines 23-24; page 4, lines 15-16; page 6, lines 25-26). The first user port can be an input port of the first edge switch (*id.*). Forwarding and routing can be determined by the first edge switch based on a user VLAN identifier (VID) of a user VLAN tag for the packet (page 1, lines 25-26, page 5, lines 2-3, 18). A tunnel can be created from the first user port at the first edge switch to a second user port at a second edge switch (page 2, lines 14-16; page 3, lines 4, 9; page 6, lines 22-26; page 7, lines 6-7, 16-17). The tunnel can be created using double VLAN tagging by inserting a provider VLAN tag, including a provider VID, into the packet at a first provider port at the first edge switch (*id.*). The provider VLAN tag can be inserted into the packet prior to transmission of the packet via the first provider port (*id.*). The provider VLAN tag can be stripped from the packet after the packet is received by a second provider port at the second edge switch (*id.*). The first provider port can be an output port of the first edge switch, and the second provider port can be an input port of the second edge switch (*id.*). Also, the second user port can be an output port of the second edge switch (*id.*). The method can further include utilizing the user VLAN tag by a middle switch to determine a class of service for the packet (page 2, lines 16-17; page 6, lines 30-33). Utilizing the user VLAN tag in this manner can provide a user-expected service level in relation to traffic flowing through said tunnel (*id.*).

In claim 11, a switch apparatus is provided for processing a packet sent to a provider network (page 1, lines 29-30). The apparatus can include a user port for

receiving the packet (page 1, lines 30-32; page 6, lines 25-26). The user port can be an input port of the switch apparatus (*id.*). The apparatus further includes forwarding logic for determining forwarding and routing based on a user VLAN identifier (VID) of a user VLAN tag for the packet (page 1, line 33-page 2 line 1; page 5, lines 2-3, 18). The forwarding logic can be used to determine a class of service based on the user VLAN tag (*id.*). A provider port can insert a provider VLAN tag, including a provider VID, into the packet prior to transmission of the packet so that the transmitted packet has at least two VLAN tags (page 2, lines 14-17; page 3, lines 4, 9; page 6, lines 22-26; page 7, lines 6-7, 16-17). The provider port can be an output port of the switch apparatus (*id.*). A tunnel can be created from the user port of the switch apparatus to another user port of a different switch apparatus by using the two VLAN tags (*id.*). A user-expected service level can be provided by the apparatus in relation to traffic flowing through said tunnel (*id.*).

In claim 12, a system is provided for processing packets sent to a provider network (page 2, lines 4-5). A first switch can receive a packet via a user port to determine routing and forwarding for the packet based on a user VID of a user VLAN tag(page 2, lines 6-9; page 3, lines 5-8; page 5, lines 6-7). The first switch can insert a provider VLAN tag into the packet at a provider port prior to transmission of the packet such that the transmitted packet has at least two VLAN tags therein (*id.*). A second switch can receive the packet having at least two VLAN tags via a provider port (page 2, lines 9-12; page 3, line 9; page 7, lines 6-7). The second switch can to strip the provider VLAN tag from the packet at the provider port and to determine routing and forwarding for the packet based on the user VID for the user VLAN tag (*id.*). A middle switch can be communicatively coupled between the first and second

switches (page 5, lines 28-31; page 6, lines 30-31; page 7, lines 3-4). A tunnel can be created between the user port of the first switch and a user port of the second switch (page 2, lines 14-16; page 7, lines 16-17). Also, a service level can be provided in relation to traffic flowing through the tunnel (page 2, lines 16-17; page 7, lines 20-23). Providing a service level in relation to traffic flowing through the tunnel can provide a security action of dropping the packet or forwarding the packet to management software (*id.*). The security action can be determined based on the user VLAN tag (page 2, lines 16-17; page 7, lines 17-21).

In claim 16, a method is provided for routing and forwarding a packet using double Q tagging (page 2, lines 13-17; page 3, lines 6-9; page 6, lines 22-24, 30-33; page 7, lines 6-7, 16-17). A provider VLAN tag can be inserted at a provider port of a first switch in addition to a user VLAN tag to create a tunnel between a user port of the first switch and a user port of a second switch (*id.*). A user-expected service level is provided in relation to traffic flowing through the tunnel by utilization of the user VLAN tag by a middle switch to determine a class of service for the packet (*id.*). The provider VLAN tag can be removed at a provider port of the second switch (*id.*).

In claim 19, an apparatus is provided for processing a packet sent to a provider network (page 1, lines 29-30). The apparatus can include means for receiving the packet via a user port of an edge switch of the network (page 1, lines 30-32; page 4, lines 15-16; page 6, lines 25-26). The user port can be an ingress port for the edge switch (*id.*). Means can be included for determining forwarding and routing by the edge switch based on a user VLAN identifier (VID) of a user VLAN tag for the packet (page 1, line 32-page 2 line 1; page 5, lines 2-3). The apparatus can include means for determining a class of service based on the user VLAN tag (*id.*). Further,

the apparatus may include means for inserting a provider VLAN tag, including a

provider VID, into the packet at a provider port of the edge switch prior to

transmission of the packet via the provider port (page 2, lines 16-17; page 3, lines 6-

10; page 6, lines 22-24; page 7, 16-17). The provider port can be an egress port of the

edge switch, such that a tunnel is created between the user port of the edge switch and

a user port of a different edge switch (*id.*). A service level can be provided in relation

to traffic flowing through said tunnel (*id.*).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for review are:

a. Whether claims 1-8, 10-11, 16, and 19 are patentable under 35 U.S.C. § 103(a) over De Silva et al. (US 2007/0110078), hereinafter De Silva, in view of the background of the invention of De Silva; and

b. Whether claims 12 and 14 are patentable under 35 U.S.C. § 103(a) over De Silva and Herren et al. (US 6,788,681) in view of the background of the invention of De Silva.

VII. ARGUMENT

A. Background

In networking and communications technology, local area networks (LANs) that are IEEE 802 compliant may be connected together with media access control (MAC) bridges. The IEEE 802.1Q standard defines the operation of virtual LAN (VLAN) bridges that permit the operation of VLANs within a bridged LAN infrastructure. In accordance with IEEE 802.1Q, data frames may be routed between ports of the VLAN according to VLAN tags. Double Q tagging, also known as double VLAN tagging, is an enhancement to IEEE 802.1Q.

B. Appellant's Method and System

Appellant's method and system facilitates efficient processing of packets sent to a provider network. As shown in FIG. 1 of the application, which has been reproduced below, various user networks are connected together with a provider's metropolitan area network.
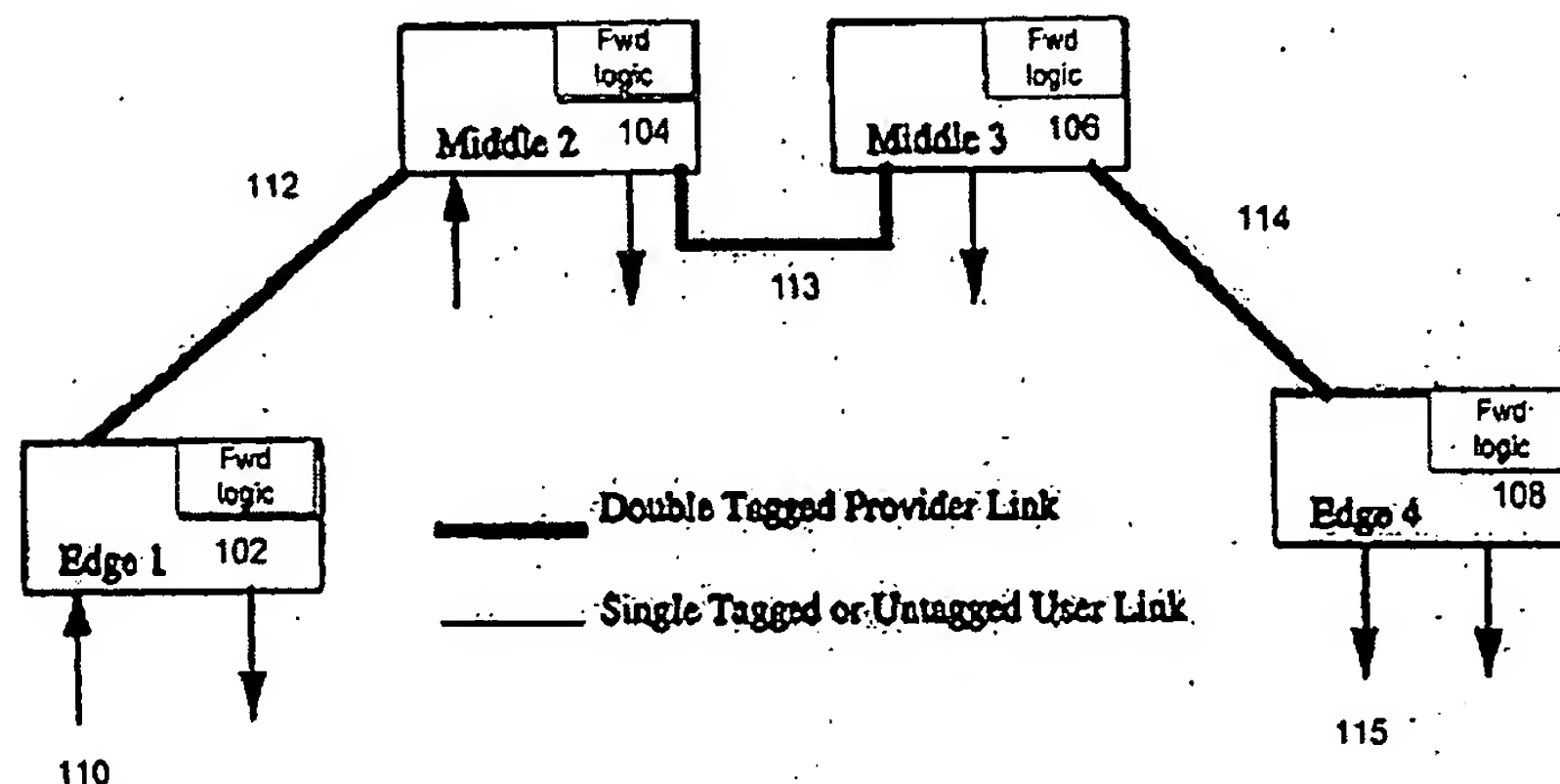

FIG. 1

A first switch 102 operates in an edge mode and receives a user packet from one

of its user links through a user port. The packet arrives at the first switch user port

with a user VLAN tag and user class of service (COS), which packet is illustrated in

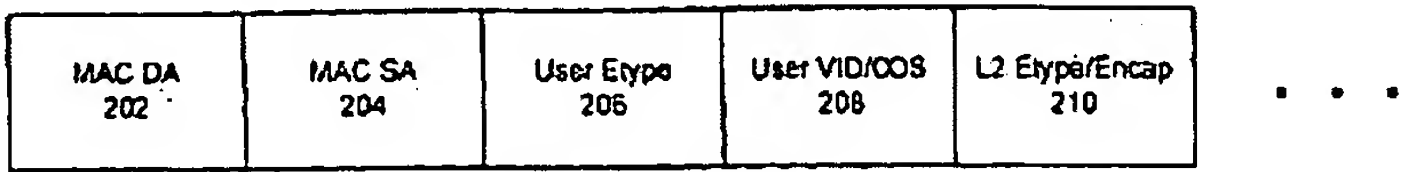FIG. 2A of the application, which has been reproduced below.

MAC DA 202	MAC SA 204	User Etype 206	User VID/COS 208	L2 Etype/Encap 210

FIG. 2A 〜 200

The forwarding logic of the first edge switch determines forwarding and routing

for the packet based on the user tag and other contents of the packet and transmits the

packet to the provider port. Then, the provider VLAN tag and provider class of

service (COS) is inserted at the provider port prior to transmission of the packet from

the provider port of the first switch through a middle switch and eventually to a

provider port of a second edge switch. The double tag of the user VLAN tag and

provider VLAN tag of the packet create a tunnel from the provider port of the first

switch to the provider port of the second switch, which double tag is illustrated in

FIG. 2B of the application, which has been reproduced below.

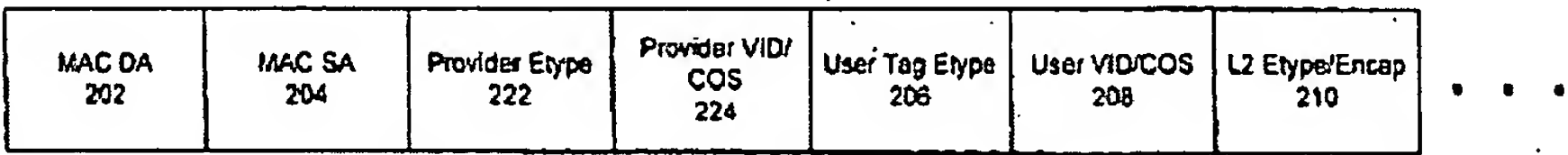| MAC DA 202	MAC SA 204	Provider Etype 222	Provider VID/ COS 224	User Tag Etype 206	User VID/COS 208	L2 Etype/Encap 210

FIG. 2B 〜 220

The tunnel efficiently transmits the packet through the middle switches of the

provider network. After the packet is received via the provider port of the second edge

switch, the provider port removes the provider tag and provider class of service

(COS). Next, forwarding logic of the second edge switch determines forwarding and

routing based on the user VLAN tag and the packet is transmitted to the user port of

the second edge switch. Finally, the packet exits via a destination user port of the

second edge switch.

Providing an insertion of the provider VLAN tag at the provider port, instead of

the user port of the first edge, switch allows the switch to route a packet from a user

port of the first switch to another user port of the same switch without the middle

switches adding a provider VLAN tag. In addition, the claimed invention provides

greater functionality for Internet Protocol (IP) multicast replication because

replication modifies the user VLAN, and the claimed invention overcomes the

inability to modify the user VLAN due to the early tagging of the provider VLAN tag

at the user port of the edge switch which adds additional overhead. Tagging and

untagging the provider VLAN tag at the provider ports reduces and eliminates the

tagging logic at the user ports of edge switches.

C.   The Asserted References

1. The De Silva Reference

De Silva discloses the connectivity of a port of a device for a customer network

to a provider network accessing a Virtual Local Area Network (VLAN) mapping data

structure. (De Silva Abstract). A schematic diagram of a computer network with

customer networks and a Metropolitan Area Network (MAN) is illustrated in FIG. 2,

which has been reproduced below.

FIG. 2
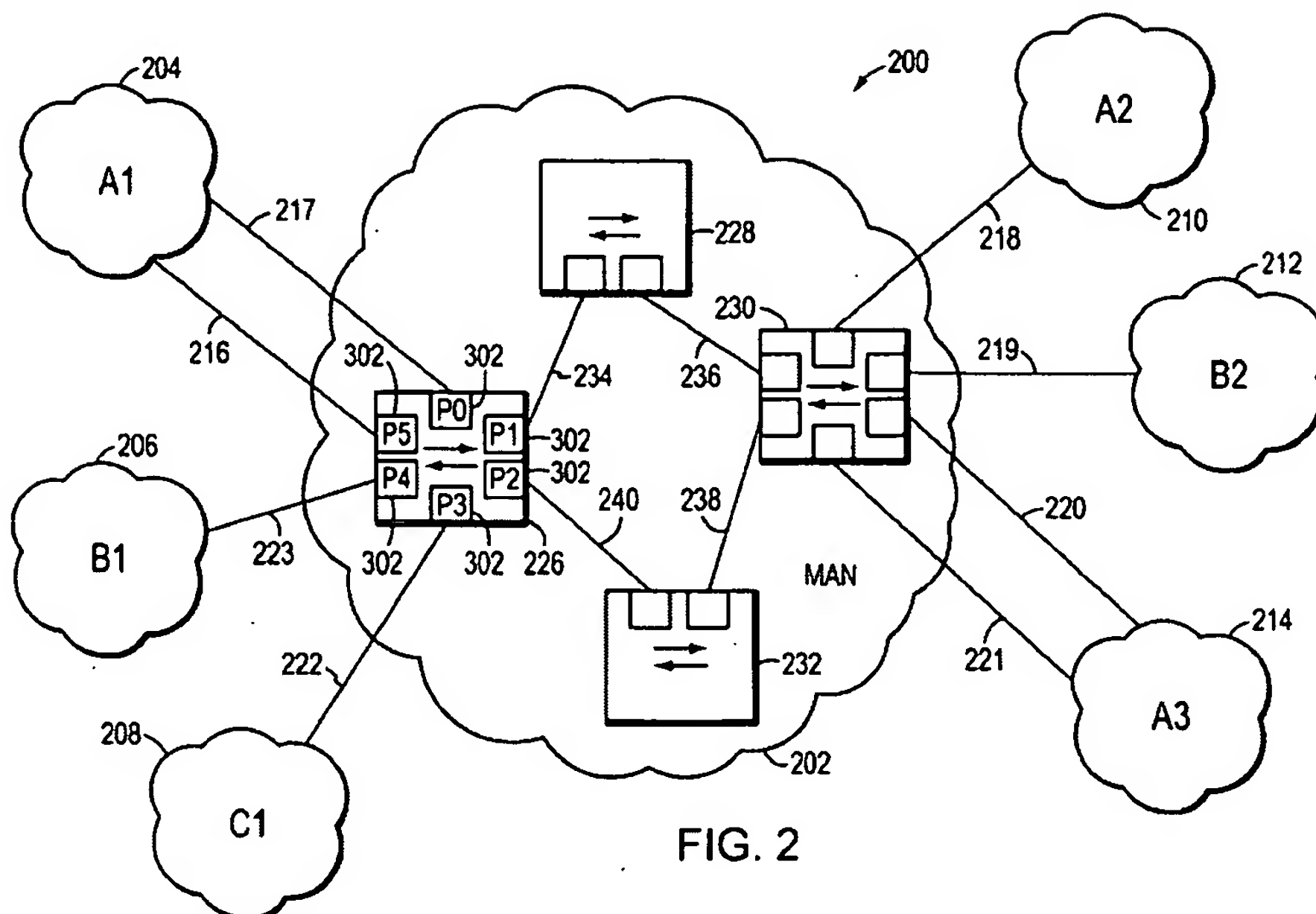
A frame 100 from a customer network is received at a customer boundary port P4

of switch 226 in MAN 202 (De Silva paragraph [0062]). Frame 100 showing user

information is illustrated in FIG. 1, which has been reproduced below.
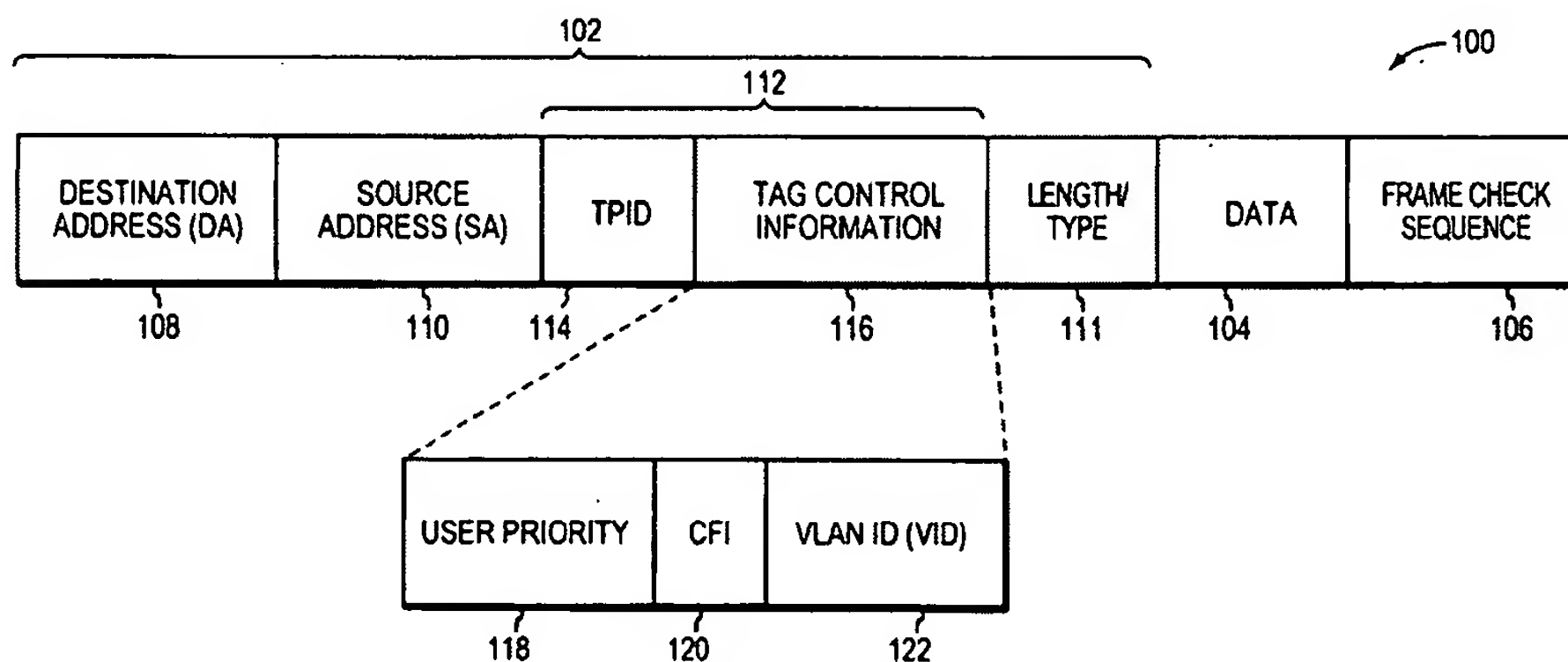
FIG. 1

Port P4 uses frame mapping logic to derive provider VLAN designations and

provider Cost of Service (CoS) values (De Silva paragraphs [0022],[0062], and

[0063]). Port P2 receives the frame from port P4 (De Silva paragraph [0064] and

[0065]). The frame mapping logic of the port P2 determines whether to append a

provider VLAN and provider Cost of Service (CoS) value to the frame 100 and their

values (De Silva paragraph [0066]). Frame 700 is formed after the provider VLAN

and provider Cost of Service (CoS) value has been appended to the frame 100, which

is illustrated in FIG. 7, which has been reproduced below (De Silva paragraph

[0070]).
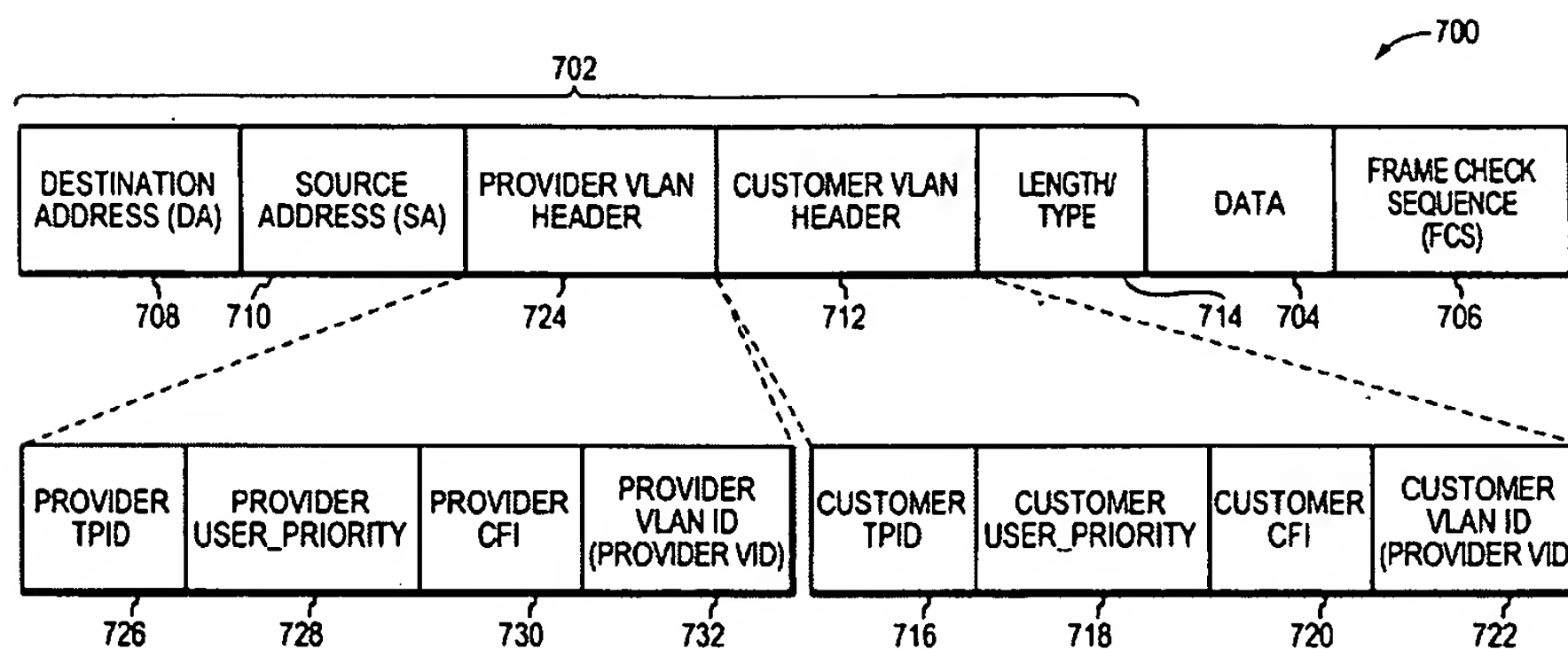
FIG. 7

Frame 700 is passed from switch 226 to an intermediate switch 232 and

eventually to a switch 230 coupled to the destination customer network (De Silva

paragraph [0078] and [0079]). When the frame is passed through the switches in the

provider network, the switches *utilize the frame's destination address (DA) and the*

appended provider frame data for prioritizing and forwarding the frame, instead of

any original user frame data (De Silva paragraph [0078]). At switch 230, the

forwarding engine determines that the provider frame 700 should be transmitted from

the outbound port, known as the port coupled to the second customer network 212

(De Silva paragraph [0080]). De Silva does not disclose the provider VLAN and

provider CoS being removed, but frame 100, which does not have the provider VLAN

and provider CoS, is transmitted into the customer network 212 (De Silva paragraph

[0081]).

De Silva removes the provider VLAN at the outbound or user port, instead

of the inbound or provider port. In addition, the intermediate switches use the

provider CoS value, instead of the user CoS value.

2. The Herren Reference

Herren discloses a method and apparatus for providing a Virtual Private Network

(VPN) over a connectionless network by connecting a plurality of Local Area

Networks (LANs) (Herren Abstract). The frame in the VPN may include a priority

field 404, which includes a discharge eligibility field 418 and a CoS indicator field,

which is illustrated in FIG. 4, which has been reproduced below (Herren column 14,
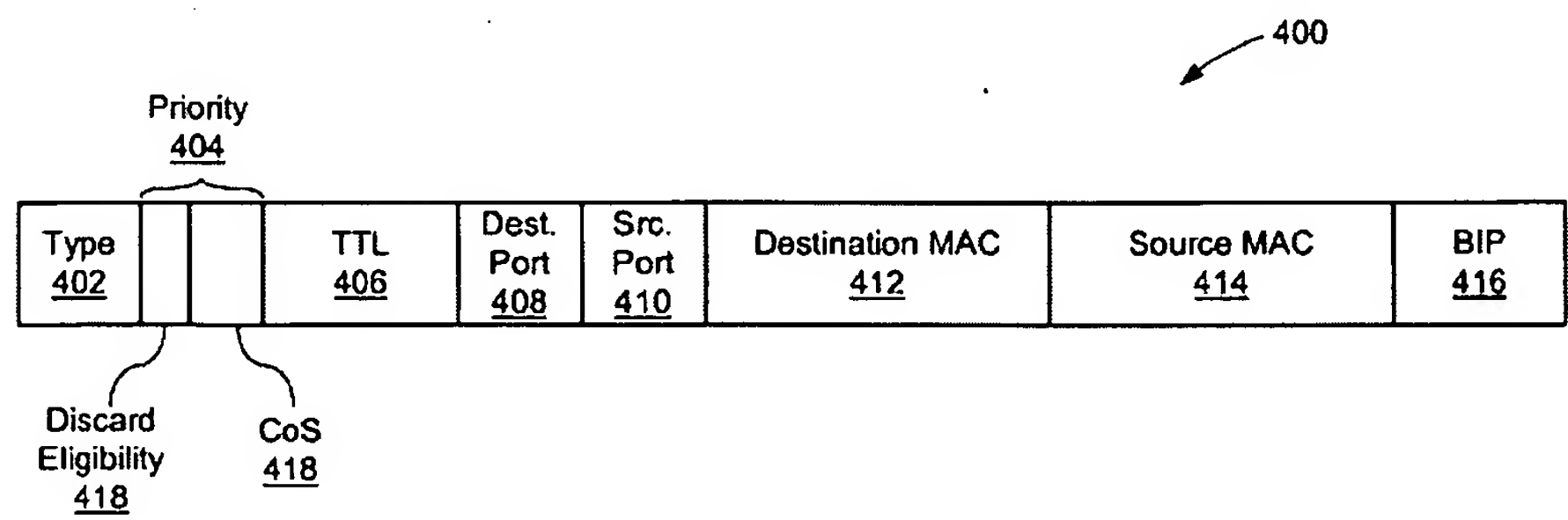
lines 55-62; FIG. 4).

FIG. 4

The discard eligibility field may allow a frame to be discarded in times of

congestion and the CoS indicator field may define up to eight classes of data (Herren

column 14, lines 55-62; FIG. 4). Congestion can occur when more frames are

received by a switch than the switch can handle. The discard eligibility field allows

packets to be dropped instead of processed and forwarded by the switch to reduce the

congestion. **The discard eligibility field is used for congestion, not security.**

D.   Rejections Under 35 U.S.C. § 103(a)

1. Requirements for Prima Facie Obviousness

The Examiner has rejected some of the pending claims under § 103(a) as being

prima facie obvious over a number of references. The Patent and Trademark Office

(PTO), through the Examiner, has the burden of establishing a *prima facie* case of

obviousness. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1998).

To satisfy this burden, the PTO must meet the criteria set out in M.P.E.P. § 706.02(j):

> [T]hree basic criteria must be met. First, there must be some suggestion or
> motivation, either in the references themselves or in the knowledge generally
> available to one of ordinary skill in the art, to modify the reference or to
> combine reference teachings. Second, there must be a reasonable
> expectation of success. Finally, the prior art reference (or references when
> combined) must teach or suggest all the claim limitations. The teaching or
> suggestion to make the claimed combination and the reasonable expectation
> of success must both be found in the prior art and not based on applicant's
> disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

An excellent summary of how the prior art must be considered to make a case of

prima facie obviousness is contained in *In re Ehrreich et al.*, 220 U.S.P.Q. 504, 509-

511 (CCPA 1979). There the court states that a reference must not be considered in a

vacuum, but against the background of the other references of record. It is stated that

the question of a § 103 case is what the reference(s) would "collectively suggest" to

one of ordinary skill in the art. However, the court specifically cautioned that the

Examiner must consider the entirety of the disclosure made by the reference and

avoid combining them indiscriminately.

In finding that the "subject matter as a whole" would not have been obvious in

Ehrreich the court concluded:

"Thus, we are directed to no combination of prior art references which would have rendered the claimed subject matter <u>as a whole</u> obvious to one of ordinary skill in the art at the time the invention was made. <u>The PTO has not shown the existence of all the claimed limitations in the prior art or any suggestion leading to their combination in the manner claimed by applicants</u>." (underlining added)

It is true that an obviousness determination is not the result of a rigid formula disassociated from the consideration of the facts of a case. Indeed, the common sense of those skilled in the art demonstrates why some combinations would have been obvious where others would not. See *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1742 (U.S. 2007). However, it has been widely recognized that virtually every invention is a combination of elements and that most, if not all, of these will be found somewhere in an examination of the prior art. This reasoning lead the court, in *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 199 (Fed. Cir. 1983) to state:

"...it is common to find elements or features somewhere in the prior art. Moreover, most if not all elements perform their ordained and expected function. The test is whether the claimed invention <u>as a whole</u>, in light of all the teachings of the references <u>in their entireties</u>, would have been obvious to one of ordinary skill in the art at the time the invention was made." (underlining added)

A showing of obviousness requires (1) some suggestion or motivation, *either in the references themselves or in the knowledge generally available to one of ordinary skill in the art*, to modify the reference or to combine reference teachings, and (2) the prior art references when combined must teach or suggest all the claim limitations (MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991))). "Analysis supporting a rejection under 35 U.S.C. § 103 should be made explicit" (memorandum from Margaret A. Focarino, Deputy Commissioner for Patent Operations to Technology Center Directors, May 3, 2007 (citing *KSR Int'l. Co. v.*

Teleflex, Inc., No 04-1350 (U.S. Apr. 30, 2007))). Moreover, in KSR the Supreme Court stated that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, *there must be some articulated reasoning with some rational underpinning* to support the legal conclusion of obviousness." *KSR*, 127 S. Ct. at 1741 (emphasis added).

With the above background in mind, Appellant contends that the Examiner has not met this burden with respect to the claims rejected under § 103. Particularly, Appellant submits that the PTO has failed to show that each and every element of the claimed invention is contained in the references. Appellant now turns to a discussion of the individual rejections at issue, and the references on which they are based.

2. The rejection of Claims 1-8, 10-11, 16, and 19 over De Silva in view of the background of the invention of De Silva

Appellant submits that the De Silva reference in view of the background of the invention of De Silva asserted by the Examiner do not teach or suggest each and every element of the rejected claims.

First, De Silva fails to disclose the removal of the provider VLAN tag at the **provider port** of the second edge switch. Second, De Silva fails to disclose that the **middle switch determines the class of service or priority for the packets using the user VLAN tag**.

As previously discussed, De Silva discloses the connectivity of a port of a device of a customer network to a provider network accessing a Virtual Local Area Network (VLAN) mapping data structure. (De Silva Abstract). The frame mapping logic of the port appends a provider VLAN and provider Cost of Service (CoS) value to the frame and transmits the frame through the MAN (De Silva paragraphs [0066] and [0078]).

At the final switch of the MAN, the provider VLAN is removed from the provider

frame 700 to regenerate the frame 100 at the outbound port or the last port before

being transmitted to the second customer network 212 (De Silva paragraph [0080]).

In contrast, independent claim 1 sets forth:

A method of processing a packet sent to a provider network, the method

comprising:

receiving the packet via a first user port at a first edge switch of the

network, wherein the first user port is an input port of the first edge switch;

determining forwarding and routing by the first edge switch based on a

user VLAN identifier (VID) of a user VLAN tag for the packet;

creating a tunnel from the first user port at the first edge switch to a

second user port at a second edge switch using double VLAN tagging by

inserting a provider VLAN tag, including a provider VID, into the packet at a

first provider port at the first edge switch prior to transmission of the packet via

the first provider port and **stripping the provider VLAN tag from the packet**

after the packet is received by a second provider port at the second edge

switch, wherein the first provider port is an output port of the first edge switch,

wherein the second provider port is an input port of the second edge switch, and

wherein the second user port is an output port of the second edge switch; and

utilizing the user VLAN tag by a middle switch to determine a class

of service for the packet so as to provide a user-expected service level in

relation to traffic flowing through said tunnel.

Regarding De Silva failing to disclose the removal of the provider VLAN tag at

the **provider port** of the second edge switch, the Examiner asserts that in paragraphs

80-81, "Switch 230 transmits original frame 100 into customer network 212, wherein

original frame 100 in Figure 1 does not include a provider VLAN tag; therefore, it is inherent that the provider VLAN tag is stripped from the packet at Switch 230" (Office Action page 4, lines 7-10). The assertion fails to distinguish between the **provider** port (or inbound port) and the **user** port (or outbound port) of switch 230. Although the provider VLAN tag is not forwarded to the customer network, De Silva suggests the user port (or outbound port) removes the tag, instead of the provider port (or inbound port). De Silva assumes the standard approach for removing the provider VLAN tag at the user or outbound port. Claim 1 overcomes the disadvantages of the standard approach suggested by De Silva by removing the provider VLAN tag at the provider port instead of the user port within the second edge switch (Application page 3, lines 18-21).

In claim 1, the provider VLAN tag is removed at the provider port in the edge switch before transmitting the frame to the user port which eventually transmits the frame without the provider VLAN tag to the customer network. In contrast, De Silva states "At switch 230, the forwarding engine determines that the **provider frame 700** should be transmitted **from the port coupled to customer network** 212. In this case, the Egress VLAN mapping table at the **outbound port of switch 230 coupled to customer network** 212" (De Silva paragraph [0080]). The entire provider frame is transmitted to the outbound port before stripping the provider VLAN tag. As suggested in De Silva, all operations and accesses to the provider frame, which includes the provider VLAN tag, occur at the outbound or user port, and not the inbound or provider port as in claim 1. From the outbound or user port, the non-provider VLAN tagged frame 100 is later transmitted into the customer network. The inbound or provider port is never mentioned in cited paragraphs [0080] and [0081], so

inherently the provider VLAN tag is removed at the outbound or user port, which

comports with the standard approach prior to the invention in claim 1.

De Silva removes the provider VLAN at the outbound or user port of the edge

switch, while claim 1 removes the provider VLAN at the inbound or provider port of

the edge switch. Remove or stripping the provider VLAN tag at the provider port is

not obvious since the industry standard approach as identified in the application is to

remove the provider VLAN tag at the user port (Application page 3, lines 18-21).

Thus, De Silva does not disclose, suggest, or teach stripping the provider VLAN tag

at the provider port as in claim 1.

Second, De Silva fails to disclose the **middle switch determining the class of**

service or priority for the packets using the user VLAN tag as in claim 1. Instead,

De Silva utilizes the provider CoS value contained in the provider user priority field

to determine which particular transmission queue should be utilized for the packet (De

Silva paragraph [0078]). The customer VLAN and CoS values are not used by the

middle switches in De Silva, and De Silva does not suggest using the customer VLAN

or CoS values.

The Examiner asserts that, "De Silva et al. teaches utilizing the user VLAN tag

by a middle switch to determine a class of service level in relation to traffic flowing

through the tunnel (see Figure 7 reference numeral 718 and paragraph 16 and 17)"

(Office Action page 4, lines 19-22). The assertion fails because the frame 100 (user

priority field 118 is only in original frame 100) of paragraph 17 is not double tagged,

which means its does not have a provider tag along with a user tag, and therefore is

not using double tagging, as in claim 1. The frame or packet in De Silva's paragraph

17 does not create a tunnel because a provider tag is missing, and the network device

must use the user tag to route the packet because the provider tag is missing from the

packet needed for a tunnel. Routing using a user tag to route and queue a single

tagged packet requires a different protocol from using a user tag to route and queue a

double tagged packet that contains both a provider and user tag. Thus, De Silva does

not disclose, suggest or teach utilizing the user VLAN tag of a tunneled packet

containing a provider VLAN tag and a user VLAN tag by a middle switch as in claim

1.

De Silva in view of the background of the invention of De Silva does not teach or

suggest each of the elements in the independent claim 1. Therefore, Appellants submit

that the rejection of independent claim 1 under § 103(a) should be overturned.

Independent claims 11, 16, and 19 have also been rejected using the same

citations and the same reasoning as in claim 1, so these independent claims should

also be overturned for the same reasons. Rejection of the dependent claims 2-8 and 10

should be reconsidered and reversed for at least the reasons given above with respect

to the independent claim. The dependent claims, being narrower in scope, are

allowable for at least the reasons for which the independent claims are allowable.

Therefore, Appellant respectfully submits that the rejection of claims 1-8, 10-12,

14, 16, and 19 under § 103(a) should be reversed.

3. The rejection of Claims 12 and 14 over De Silva and Herren in view of the background of the invention of De Silva

Appellant submits that the addition of Herren does not overcome the deficiencies

of De Silva as to teach or suggest each and every element of the rejected claims 12

and 14. Specifically, and as previously discussed in relation to claim 1, Herren fails

teach "to strip the provider VLAN tag from the packet at the provider port," and

"wherein the security action is determined based on the user VLAN tag" as is claimed

in claim 12. In addition, neither De Silva nor Herren teach or suggest "wherein a

service level is provided in relation to traffic flowing through said tunnel which

provides a security action of dropping the packet or forwarding the packet to

management software," as claimed in claim 12 and it would not be obvious to a

person skilled in the arts to do so.

As previously discussed, Herren discloses a method and apparatus for providing

a Virtual Private Network (VPN) over a connectionless network by connecting a

plurality of Local Area Networks (LANs) (Herren Abstract). The frame in the VPN

may include a priority field 404, which includes a discharge eligibility field 418 and a

CoS indicator field (Herren column 14, lines 55-62; FIG. 4). The discard eligibility

field may allow a frame to be discarded in times of congestion and the CoS indicator

field may define up to eight classes of data (Herren column 14, lines 55-62; FIG. 4).

In contrast, independent claim 12 sets forth:

A system for processing packets sent to a provider network, the system

comprising:

a first switch configured to receive a packet via a user port, to determine

routing and forwarding for the packet based on a user VID of a user VLAN tag,

and to insert a provider VLAN tag into the packet at a provider port prior to

transmission of the packet such that the transmitted packet has at least two

VLAN tags therein;

a second switch configured to receive the packet having at least two

VLAN tags via a provider port, **to strip the provider VLAN tag from the**

packet at the provider port, and to determine routing and forwarding for the

packet based on the user VID for the user VLAN tag; and

a middle switch communicatively coupled between the first and second

switches,

wherein a tunnel is created between the user port of the first switch and a

user port of the second switch, and

wherein a **service level** is provided in relation to traffic flowing through

said tunnel which provides a **security action of dropping the packet or**

forwarding the packet to management software,

wherein the **security action is determined based on the user VLAN**

tag.

Herren fails to disclose a security action of dropping the packet or forwarding the

packet to management software for further analysis as claimed in claim 12

(Application page 7, line 23). Instead, Herren discloses a discard eligibility field to

discard a packet where congestion occurs (Herren column 14, lines 55-62). Dropping

packets due to congestion differs in functionality from dropping packets for security

issues and uses different logic. For example, if an excessive number of packets are

sent to a network device, an enabled discard eligibility field on some of the packets

may cause those packets to be discarded when the network device exceeds a threshold

congestion level to relieve the congestion. In contrast, a security action may evaluate

the packet contents based on a service level and a packet threat model, which

indicates packets that could jeopardize the security and stability of the network

device. The security action can drop a suspect packet to eliminate the security threat,

regardless of congestion levels. A discard eligibility field is not a security action or

mechanism, and a discard eligibility field does not generate a security action as in

claim 12. In addition, Herren fails to disclose a security action relative to the frame,

and it would not be obvious to do so as asserted by the Examiner. Congestion and security are both problems associated with networks, but each problem uses different and distinct solutions. Moreover, Herren fails to disclose forwarding the packet to management software for further analysis. Thus, Herren fails to disclose a security action of dropping the packet or forwarding the packet to management software as claimed in claim 12.

Thus, the combination of De Silva and Herren do not teach or suggest each of the elements in the independent claim 12. Therefore, Appellants submit that the rejection of independent claim 12 under § 103(a) should be overturned.

Rejection of the dependent claim 14 should be reconsidered and reversed for at least the reasons given above with respect to the independent claim 12. The dependent claims, being narrower in scope, are allowable for at least the reasons for which the independent claims are allowable.

Therefore, Appellant submits that the rejection of claims 12 and 14 under §103(a) should be reversed.

E. Conclusion

Appellant respectfully submits that the claims on appeal set forth in the Appendix

are patentably distinct from the asserted prior art references. Particularly, none of the

asserted combinations of references motivates, teaches, or suggests one of ordinary

skill in the art within the meaning of 35 U.S.C. § 103(a) to arrive at the presently

claimed invention. Appellant contends that De Silva in view of the background of the

invention of De Silva fails to teach each and every element of the claimed invention.

The same contentions apply to the combination of De Silva and Herren in view of the

background of the invention of De Silva.

For these reasons, Appellant respectfully requests that the Board of Appeals

reverse the rejection and remand the case to the Examiner for allowance.

Dated this 27th day of April, 2009:

/Steve M. Perry/
_____
Steve M. Perry
Attorney for Appellant
Registration No. 45,357

THORPE NORTH & WESTERN, LLP
8180 South 700 East, Suite 200
Sandy, Utah 84070
(801) 566-6633

On Behalf Of:
HEWLETT-PACKARD DEVELOPMENT
COMPANY
20555 S.H. 249
Houston, TX 77070

VIII. CLAIMS APPENDIX

1. A method of processing a packet sent to a provider network, the method comprising:

   receiving the packet via a first user port at a first edge switch of the network, wherein the first user port is an input port of the first edge switch;

   determining forwarding and routing by the first edge switch based on a user VLAN identifier (VID) of a user VLAN tag for the packet;

   creating a tunnel from the first user port at the first edge switch to a second user port at a second edge switch using double VLAN tagging by inserting a provider VLAN tag, including a provider VID, into the packet at a first provider port at the first edge switch prior to transmission of the packet via the first provider port and stripping the provider VLAN tag from the packet after the packet is received by a second provider port at the second edge switch, wherein the first provider port is an output port of the first edge switch, wherein the second provider port is an input port of the second edge switch, and wherein the second user port is an output port of the second edge switch; and

   utilizing the user VLAN tag by a middle switch to determine a class of service for the packet so as to provide a user-expected service level in relation to traffic flowing through said tunnel.

2. The method of claim 1, further comprising:

   forwarding and routing the packet by a middle switch based on the provider VLAN tag.

3. The method of claim 1, wherein the packet received includes the user VLAN tag, and wherein the user VID is derived from the user VLAN tag.

4. The method of claim 1, wherein the packet received does not include a user VLAN tag, and wherein the user VID is assigned to be a port VID associated with the user port.

5. The method of claim 1, wherein the provider VID comprises a VID of a destination VLAN.

6. The method of claim 1, wherein the provider VID comprises a port VID associated with the input port.

7. The method of claim 1, wherein the first edge switch also determines the class of service for the packet based on the user VLAN tag.

8. The method of claim 1, wherein the first edge switch determines the security action for the packet based on the user VLAN tag.

9. Canceled.

10. The method of claim 1, wherein the packet is routed to more than one middle switch before arriving at the second edge switch.

11. A switch apparatus for processing a packet sent to a provider network, the apparatus comprising:

> a user port for receiving the packet, the user port being an input port of the switch apparatus;

> forwarding logic for determining forwarding and routing based on a user VLAN identifier (VID) of a user VLAN tag for the packet, including determination of a class of service based on the user VLAN tag; and

> a provider port that inserts a provider VLAN tag, including a provider VID, into the packet prior to transmission of the packet such that the transmitted packet has at least two VLAN tags, the provider port being an output port of the switch apparatus, such that a tunnel is created from the user port of the switch apparatus to another user port of a different switch apparatus, wherein a user-expected service level is provided in relation to traffic flowing through said tunnel.

12. A system for processing packets sent to a provider network, the system comprising:

> a first switch configured to receive a packet via a user port, to determine routing and forwarding for the packet based on a user VID of a user

VLAN tag, and to insert a provider VLAN tag into the packet at a

provider port prior to transmission of the packet such that the

transmitted packet has at least two VLAN tags therein;

a second switch configured to receive the packet having at least two VLAN

tags via a provider port, to strip the provider VLAN tag from the

packet at the provider port, and to determine routing and forwarding

for the packet based on the user VID for the user VLAN tag; and

a middle switch communicatively coupled between the first and second

switches,

wherein a tunnel is created between the user port of the first switch and a user

port of the second switch, and

wherein a service level is provided in relation to traffic flowing through said

tunnel which provides a security action of dropping the packet or

forwarding the packet to management software,

wherein the security action is determined based on the user VLAN tag.

13. Canceled.

14. The system of claim 12, further comprising utilization of a class of service (COS)
for routing and forwarding of the packet that is based on the user VID.

15. Canceled.

16. A method of routing and forwarding a packet using double Q tagging by inserting
a provider VLAN tag at a provider port of a first switch in addition to a user
VLAN tag to create a tunnel between a user port of the first switch and a user
port of a second switch, wherein a user-expected service level is provided in
relation to traffic flowing through the tunnel by utilization of the user VLAN tag
by a middle switch to determine a class of service for the packet, and wherein the
provider VLAN tag is removed at a provider port of the second switch.

17. Canceled.

18. Canceled.

19. An apparatus for processing a packet sent to a provider network, the apparatus comprising:

      means for receiving the packet via a user port of an edge switch of the network, the user port being an ingress port for the edge switch;

      means for determining forwarding and routing by the edge switch based on a user VLAN identifier (VID) of a user VLAN tag for the packet and for determining a class of service based on the user VLAN tag; and

      means for inserting a provider VLAN tag, including a provider VID, into the packet at a provider port of the edge switch prior to transmission of the packet via the provider port, the provider port being an egress port of the edge switch, such that a tunnel is created between the user port of the edge switch and a user port of a different edge switch, wherein a service level is provided in relation to traffic flowing through said tunnel.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None